Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1-31. (canceled)

33. (previously presented) A method of establishing a secure communication channel, comprising:

sending, by a first party, a secure call notification to a second party;

accessing, by the first and second parties, base, prime, and sub-prime parameters;

generating, by the second party, a second asymmetric key pair comprising a second public key and a second private key, based on the base, prime, and sub-prime parameters;

sending, by the second party to the first party, the second public key;

generating, by the first party, a net label, a private label, a random value, a first asymmetric key pair comprising a first public key and a first private key based on the base, prime, and sub-prime parameters, and a shared key based on the second public key;

encrypting, by the first party, the net label, the private label, and the random value, using the shared key;

sending, by the first party to the second party, the encrypted net label, the encrypted private label, the encrypted random value, and the first public key;

generating, by the second party, the shared key based on the first public key;

decrypting, by the second party, the encrypted net label, the encrypted private label, and the encrypted random value using the shared key; and

exchanging, by the first and second parties, respective identification numbers to establish the secure communication channel.

34. (previously presented) The method of claim 33, wherein the secure call notification is a first secure call notification, the net label is a first net label, the private label is a first private label, the random value is a first random value, the shared key is a first shared key, the encrypted net label is a first encrypted first net label, the encrypted private label is a first encrypted first private label, and the encrypted random value is a first encrypted first random value further, the method further comprising:

designating, by one of the first party and the second party, either of the first party and the second party as a sender, and the other of the first party and the second party as a non-sender;

suspending, by the sender, the secure communication channel between the first party and the second party;

establishing, by the sender, a communication channel with a third party;

sending, by the sender, a second secure call notification to the third party;

accessing, by the third party, the base, prime, and sub-prime parameters;

generating, by the third party, a third asymmetric key pair comprising a third private key and a third public key, based on the base, prime, and sub-prime parameters;

sending, by the third party to the sender, the third public key;

generating, by the sender, a second private label, a second net label, a second random value, a fourth asymmetric key pair comprising a fourth public key and a fourth private key based on the base, prime, and sub-prime parameters, and a second shared key based on the third public key;

encrypting, by the sender, the second private label, the first net label, and the first random value, using the second shared key, to provide an encrypted second private label, a second encrypted first net label, and a second encrypted first random value;

sending, by the sender to the third party, the encrypted second private label, the second encrypted first net label, the second encrypted first random value, and the fourth public key;

generating, by the third party, the second shared key based on the third public key;

decrypting, by the third party, the encrypted second private label, the second encrypted first net label, and the second encrypted first random value, using the second shared key;

suspending, by the sender, the secure communication channel between the sender and the third party;

sending, by the sender to the third party and the non-sender, a conference call notification;

encrypting, by the sender, the second net label and the second random value, using one of the first public key and the second public key, to provide a first encrypted second net label and a first encrypted second random value;

generating, by the sender, a first error detection value for the first encrypted second net label and the first encrypted second random value;

sending, by the sender to the non-sender, the first encrypted second net label, the first encrypted second random value, and the first error correction value;

generating, by the non-sender, a second error detection value, for the first encrypted second net label and the first encrypted second random value;

checking, by the non-sender, the validity of the first encrypted second net label and the first encrypted second random value by comparing the first and second error detection values;

decrypting, by the non-sender, the first encrypted second net label and the first encrypted second random value, using one of the first private key and the second private key;

encrypting, by the sender, the second net label and the second random value, using the third public key, to provide a second encrypted second net label and a second encrypted second random value;

generating, by the sender, a third error detection value, for the second encrypted second net label and the second encrypted second random value;

sending, by the sender to the third party, the second encrypted second net label, the second encrypted second random value, and the third error correction value;

generating, by the third party, a fourth error detection value, for the second encrypted second net label and the second encrypted second random value;

checking, by the third party, the validity of the second encrypted second net label and the second encrypted second random value by comparing the third and fourth error detection values; and

decrypting, by the third party, the second encrypted second net label and the second encrypted second random value, using third private key.

35. (previously presented) A method of establishing a secure communication channel, comprising:

establishing a communication link among at least three parties comprising a first party and other parties;

sending, by the first party, a broadcast conference call notification to the other parties;

accessing, by the first party and the other parties, base, prime, and sub-prime parameters;

generating, by the first party, a net label, a random value, and a first asymmetric key pair comprising a first public key and a first private key based on the base, prime, and sub-prime parameters;

sending, by the first party, the first public key to each of the other parties;

generating, by each of the other parties, a respective private label, a respective other asymmetric key pair comprising a respective other public key and a respective other private key based on the base, prime, and sub-prime parameters, and a respective other shared key based on the first public key;

encrypting, by each of the other parties, the respective private label using the respective shared key;

sending, by each of the other parties, the respective encrypted private label and the respective other public key to the first party;

computing, by the first user, each respective shared key from each respective public key sent by the other parties;

decrypting, by the first party, each respective encrypted private label using the respective shared keys;

respectively encrypting, by the first user, the net label and the random number, using the respective shared keys;

sending, by the first party, the respective encrypted net labels and the respective encrypted random values to the respective other parties;

decrypting, by the other parties, the respective encrypted net labels and the respective encrypted random values using the respective shared keys; and

establishing, by the first user and the other users, the secure communication channel using the net label and the random value.

36. (previously presented) The method of claim 35, further comprising:

deriving, by the first party, an error checking code for each of the respective other parties from the respective encrypted net labels and the respective encrypted random values;

sending, by the first party, the respective error checking codes to the respective other parties; and

confirming, by the other parties, validity of the respective encrypted net labels and the respective encrypted random values using the respective error checking codes.

37-41. (canceled)